AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions, listing, of claims in the specification.

Listing of Claims:

Claim 1. (Currently Amended) A method of key-management in Distributed Sensor Networks, comprising the steps of:

prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing a respective key ring including a plurality of individually selectable private keys in each sensor node of the Distributed Sensor Network, said private keys being randomly chosen from a common pool, said key rings of at least a pair of said sensor nodes having a pre-defined probability of having at least one private key in common;

wherein the step of storing a respective key ring further includes the steps of:

generating a key space having a multiplicity of keys,

randomly selecting a pool of keys from said key space,

assigning a specific key identifier for each key in said pool of keys,

randomly selecting a number of the keys from said pool of keys to form said respective key ring for each sensor node, said number of keys being probabilistically determined to provide said pre-defined probability of said pair of sensor nodes having at least one shared private key, and

storing said specific key identifier with said respective key ring in each said sensor node;

deploying said plurality of the sensor nodes of the Distributed Sensor Network;

actuating at least one sensor node to discover at least another sensor node sharing said at least one private key to establish a secure communication link between said one sensor node and another of said sensor nodes; and

using said at least one shared private key for subsequent secure communication between said at least one sensor node and said other sensor node.

Claim 2. (Canceled)

Claim 3. (Currently Amended) The method of claim 1 [[2]], wherein the step of deploying is preceded by the step of: assigning to each said sensor node a specific sensor identifier.

Claim 4. (Previously Presented) The method of claim 3, where the step of actuating includes the step of: broadcasting said key identifiers with said specific sensor identifier associated with said at least one sensor node to discover said at least another sensor node and establish a link therewith.

Claim 5. (Previously Presented) The method of claim 3, wherein the step of deploying is preceded by the steps of:

providing a controller node to securely communicate with a plurality of said sensor nodes for collecting data therefrom;

storing said key identifiers of the keys in said respective key ring of each said sensor node along with said sensor identifier of said each sensor node on said controller node.

Claim 6. (Original) The method of claim 4, wherein said key identifiers are broadcast in a clear text.

Claim 7. (Original) The method of claim 4, wherein said key identifiers are broadcast in a hidden pattern.

Claim 8. (Previously Presented) The method of claim 5, further comprising the steps of: computing a plurality of sensor-controller keys respectively shared by said plurality of sensor nodes with said controller node, and loading said controller node and each of said sensor nodes with an associated one of said sensor-controller keys.

Claim 9. (Previously Presented) The method of claim 5, further comprising the steps of: upon compromising of at least one sensor node, revoking said at least one compromised sensor node by broadcasting from said controller node a revocation message containing a signed list of the key identifiers of the key ring of said compromised sensor node to be revoked.

Claim 10. (Original) The method of claim 9, further comprising the steps of: generating a signature key for said list and unicasting the same to each said sensor node.

Claim 11. (Original) The method of claim 10, further comprising the steps of: upon obtaining of said signature key by an uncompromised sensor node, verifying said signature key of said signed list of the key identifiers of the key ring of said compromised sensor node, locating said key identifiers in said key ring of said uncompromised sensor node, and removing keys corresponding to the key identifiers of the compromised keys from said key ring of said uncompromised sensor node.

Claim 12. (Original) The method of claim 9, further comprising the steps of: reconfiguring the communication links of the sensor nodes affected by revocation of said compromised sensor node.

Claim 13. (Previously Presented) The method of claim 1, further comprising the steps of: upon expiration of at least one key shared by said at least one and the other sensor node, removal of said expired at least one key from said key rings of said at least one and the other sensor nodes, and searching for another key common for said at least one and the other sensor nodes to establish a new communication link therebetween.

Claim 14. (Currently Amended) The method of claim 1 [[2]], further comprising the steps of: generating a connectivity random graph for said Distributed Sensor Network, and computing the number of the sensor nodes, the number of keys in said pool of keys and the size of each said key ring, sufficient to provide for a connected Distributed Sensor Network.

Claim 15. (Original) The method of claim 1, further comprising the step of: assigning a path-key to a selected pair of sensor nodes connected by at least two communication links.

Claim 16. (Currently Amended) A Distributed Sensor Network system, comprising:

at least two sensor nodes, each said sensor node being pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys randomly chosen from a common pool, the key rings of at least a pair of said sensor nodes having a pre-defined probability of having at least one private key in common, each of said private keys of said key ring having an associated key identifier stored in a corresponding sensor node; ~~and~~ each of said sensor nodes having means for searching for another sensor node where a plurality of said key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, said matching key identifier indicating the other sensor node has a private key in common therewith to establish a secure communication link therebetween;

means for generating a key space having a multiplicity of keys, means for randomly selecting a pool of keys from said key space, means for assigning a specific key identifier for each key of said pool of keys, and means for randomly selecting a distinct set of private keys from said pool of keys for each said sensor node to thereby form said respective key rings for said sensor nodes.

Claim 17-18 (Canceled).

Claim 19. (Currently Amended) The Distributed Sensor Network system of claim 16 [[17]], further comprising: at least one controller node for secure communication with at least one of sensor nodes, said at least one controller node having said key identifiers of said key ring of said at least one sensor node and a specific sensor identifier of said at least one sensor node saved therein, and a sensor-controller key stored therein and respectively stored in a corresponding sensor node.

Claim 20. (Original) The Distributed Sensor Network system of claim 19, further comprising means for generating a revocation message and broadcasting the same for revocation of a compromised at least one of said two sensor nodes, said revocation message containing a signed list of said key identifiers of said key ring of said compromised sensor node.

Claim 21. (Original) The Distributed Sensor Network system of claim 20, further comprising means for reconfiguring communication links of said at least another sensor node affected by revocation of said compromised sensor node.

Claim 22. (Previously Presented) The Distributed Sensor Network system of claim 16, further comprising means for assigning a path-key to a selected pair of sensor nodes connected by at least two communication links.